UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

NOTICE OF ALLOWANCE AND FEE(S) DUE

45209 7590 04/03/2009

INTEL/BSTZ
BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
SHAN, APRIL YING	
ART UNIT	PAPER NUMBER
2435	

DATE MAILED: 04/03/2009

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/715,970	11/17/2003	Sundeep M. Bajikar	42.P18073	5365

TITLE OF INVENTION: METHOD AND SYSTEM TO PROVIDE A TRUSTED CHANNEL WITHIN A COMPUTER SYSTEM FOR A SIM DEVICE

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1510	$300	$0	$1810	07/06/2009

THE APPLICATION IDENTIFIED ABOVE HAS BEEN EXAMINED AND IS ALLOWED FOR ISSUANCE AS A PATENT. PROSECUTION ON THE MERITS IS CLOSED. THIS NOTICE OF ALLOWANCE IS NOT A GRANT OF PATENT RIGHTS. THIS APPLICATION IS SUBJECT TO WITHDRAWAL FROM ISSUE AT THE INITIATIVE OF THE OFFICE OR UPON PETITION BY THE APPLICANT. SEE 37 CFR 1.313 AND MPEP 1308.

THE ISSUE FEE AND PUBLICATION FEE (IF REQUIRED) MUST BE PAID WITHIN THREE MONTHS FROM THE MAILING DATE OF THIS NOTICE OR THIS APPLICATION SHALL BE REGARDED AS ABANDONED. THIS STATUTORY PERIOD CANNOT BE EXTENDED. SEE 35 U.S.C. 151. THE ISSUE FEE DUE INDICATED ABOVE DOES NOT REFLECT A CREDIT FOR ANY PREVIOUSLY PAID ISSUE FEE IN THIS APPLICATION. IF AN ISSUE FEE HAS PREVIOUSLY BEEN PAID IN THIS APPLICATION (AS SHOWN ABOVE), THE RETURN OF PART B OF THIS FORM WILL BE CONSIDERED A REQUEST TO REAPPLY THE PREVIOUSLY PAID ISSUE FEE TOWARD THE ISSUE FEE NOW DUE.

HOW TO REPLY TO THIS NOTICE:

I. Review the SMALL ENTITY status shown above.

If the SMALL ENTITY is shown as YES, verify your current SMALL ENTITY status:

A. If the status is the same, pay the TOTAL FEE(S) DUE shown above.

B. If the status above is to be removed, check box 5b on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and twice the amount of the ISSUE FEE shown above, or

If the SMALL ENTITY is shown as NO:

A. Pay TOTAL FEE(S) DUE shown above, or

B. If applicant claimed SMALL ENTITY status before, or is now claiming SMALL ENTITY status, check box 5a on Part B - Fee(s) Transmittal and pay the PUBLICATION FEE (if required) and 1/2 the ISSUE FEE shown above.

II. PART B - FEE(S) TRANSMITTAL, or its equivalent, must be completed and returned to the United States Patent and Trademark Office (USPTO) with your ISSUE FEE and PUBLICATION FEE (if required). If you are charging the fee(s) to your deposit account, section "4b" of Part B - Fee(s) Transmittal should be completed and an extra copy of the form should be submitted. If an equivalent of Part B is filed, a request to reapply a previously paid issue fee must be clearly made, and delays in processing may occur due to the difficulty in recognizing the paper as an equivalent of Part B.

III. All communications regarding this application must give the application number. Please direct all communications prior to issuance to Mail Stop ISSUE FEE unless advised to the contrary.

IMPORTANT REMINDER: Utility patents issuing on applications filed on or after Dec. 12, 1980 may require payment of maintenance fees. It is patentee's responsibility to ensure timely payment of maintenance fees when due.

PTOL-85 (Rev. 08/07) Approved for use through 08/31/2010.

PART B - FEE(S) TRANSMITTAL

Complete and send this form, together with applicable fee(s), to: Mail **Mail Stop ISSUE FEE**
Commissioner for Patents
P.O. Box 1450
Alexandria, Virginia 22313-1450
or Fax (571)-273-2885

INSTRUCTIONS: This form should be used for transmitting the ISSUE FEE and PUBLICATION FEE (if required). Blocks 1 through 5 should be completed where appropriate. All further correspondence including the Patent, advance orders and notification of maintenance fees will be mailed to the current correspondence address as indicated unless corrected below or directed otherwise in Block 1, by (a) specifying a new correspondence address; and/or (b) indicating a separate "FEE ADDRESS" for maintenance fee notifications.

CURRENT CORRESPONDENCE ADDRESS (Note: Use Block 1 for any change of address)

45209 7590 04/03/2009

INTEL/BSTZ
BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

Note: A certificate of mailing can only be used for domestic mailings of the Fee(s) Transmittal. This certificate cannot be used for any other accompanying papers. Each additional paper, such as an assignment or formal drawing, must have its own certificate of mailing or transmission.

Certificate of Mailing or Transmission

I hereby certify that this Fee(s) Transmittal is being deposited with the United States Postal Service with sufficient postage for first class mail in an envelope addressed to the Mail Stop ISSUE FEE address above, or being facsimile transmitted to the USPTO (571) 273-2885, on the date indicated below.

(Depositor's name)
(Signature)
(Date)

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/715,970	11/17/2003	Sundeep M. Bajikar	42.P18073	5365

TITLE OF INVENTION: METHOD AND SYSTEM TO PROVIDE A TRUSTED CHANNEL WITHIN A COMPUTER SYSTEM FOR A SIM DEVICE

APPLN. TYPE	SMALL ENTITY	ISSUE FEE DUE	PUBLICATION FEE DUE	PREV. PAID ISSUE FEE	TOTAL FEE(S) DUE	DATE DUE
nonprovisional	NO	$1510	$300	$0	$1810	07/06/2009

EXAMINER	ART UNIT	CLASS-SUBCLASS
SHAN, APRIL YING	2435	713-171000

1. Change of correspondence address or indication of "Fee Address" (37 CFR 1.363).

❑ Change of correspondence address (or Change of Correspondence Address form PTO/SB/122) attached.

❑ "Fee Address" indication (or "Fee Address" Indication form PTO/SB/47; Rev 03-02 or more recent) attached. **Use of a Customer Number is required.**

2. For printing on the patent front page, list

(1) the names of up to 3 registered patent attorneys or agents OR, alternatively,

(2) the name of a single firm (having as a member a registered attorney or agent) and the names of up to 2 registered patent attorneys or agents. If no name is listed, no name will be printed.

1 _____

2 _____

3 _____

3. ASSIGNEE NAME AND RESIDENCE DATA TO BE PRINTED ON THE PATENT (print or type)

PLEASE NOTE: Unless an assignee is identified below, no assignee data will appear on the patent. If an assignee is identified below, the document has been filed for recordation as set forth in 37 CFR 3.11. Completion of this form is NOT a substitute for filing an assignment.

(A) NAME OF ASSIGNEE (B) RESIDENCE: (CITY and STATE OR COUNTRY)

Please check the appropriate assignee category or categories (will not be printed on the patent) : ❑ Individual ❑ Corporation or other private group entity ❑ Government

4a. The following fee(s) are submitted:

❑ Issue Fee

❑ Publication Fee (No small entity discount permitted)

❑ Advance Order - # of Copies _____

4b. Payment of Fee(s): **(Please first reapply any previously paid issue fee shown above)**

❑ A check is enclosed.

❑ Payment by credit card. Form PTO-2038 is attached.

❑ The Director is hereby authorized to charge the required fee(s), any deficiency, or credit any overpayment, to Deposit Account Number _____ (enclose an extra copy of this form).

5. **Change in Entity Status** (from status indicated above)

❑ a. Applicant claims SMALL ENTITY status. See 37 CFR 1.27.

❑ b. Applicant is no longer claiming SMALL ENTITY status. See 37 CFR 1.27(g)(2).

NOTE: The Issue Fee and Publication Fee (if required) will not be accepted from anyone other than the applicant; a registered attorney or agent; or the assignee or other party in interest as shown by the records of the United States Patent and Trademark Office.

Authorized Signature _____ Date _____

Typed or printed name _____ Registration No. _____

This collection of information is required by 37 CFR 1.311. The information is required to obtain or retain a benefit by the public which is to file (and by the USPTO to process) an application. Confidentiality is governed by 35 U.S.C. 122 and 37 CFR 1.14. This collection is estimated to take 12 minutes to complete, including gathering, preparing, and submitting the completed application form to the USPTO. Time will vary depending upon the individual case. Any comments on the amount of time you require to complete this form and/or suggestions for reducing this burden, should be sent to the Chief Information Officer, U.S. Patent and Trademark Office, U.S. Department of Commerce, P.O. Box 1450, Alexandria, Virginia 22313-1450. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, Virginia 22313-1450.

Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/715,970	11/17/2003	Sundeep M. Bajikar	42.P18073	5365

45209 7590 04/03/2009

INTEL/BSTZ
BLAKELY SOKOLOFF TAYLOR & ZAFMAN LLP
1279 OAKMEAD PARKWAY
SUNNYVALE, CA 94085-4040

EXAMINER	
SHAN, APRIL YING	
ART UNIT	PAPER NUMBER
2435	

DATE MAILED: 04/03/2009

Determination of Patent Term Adjustment under 35 U.S.C. 154 (b)

(application filed on or after May 29, 2000)

The Patent Term Adjustment to date is 623 day(s). If the issue fee is paid on the date that is three months after the mailing date of this notice and the patent issues on the Tuesday before the date that is 28 weeks (six and a half months) after the mailing date of this notice, the Patent Term Adjustment will be 623 day(s).

If a Continued Prosecution Application (CPA) was filed in the above-identified application, the filing date that determines Patent Term Adjustment is the filing date of the most recent CPA.

Applicant will be able to obtain more detailed information by accessing the Patent Application Information Retrieval (PAIR) WEB site (http://pair.uspto.gov).

Any questions regarding the Patent Term Extension or Adjustment determination should be directed to the Office of Patent Legal Administration at (571)-272-7702. Questions relating to issue and publication fee payments should be directed to the Customer Service Center of the Office of Patent Publication at 1-(888)-786-0101 or (571)-272-4200.

PTOL-85 (Rev. 08/07) Approved for use through 08/31/2010.

Notice of Allowability	Application No.	Applicant(s)	
	10/715,970	BAJIKAR, SUNDEEP M.	
	Examiner	Art Unit	
	APRIL Y. SHAN	2435	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address--

All claims being allowable, PROSECUTION ON THE MERITS IS (OR REMAINS) CLOSED in this application. If not included herewith (or previously mailed), a Notice of Allowance (PTOL-85) or other appropriate communication will be mailed in due course. **THIS NOTICE OF ALLOWABILITY IS NOT A GRANT OF PATENT RIGHTS.** This application is subject to withdrawal from issue at the initiative of the Office or upon petition by the applicant. See 37 CFR 1.313 and MPEP 1308.

1. ☒ This communication is responsive to *28 January 2009*.

2. ☒ The allowed claim(s) is/are *1,3-6,8-13,15-25 and 29*.

3. ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
   a) ☐ All b) ☐ Some* c) ☐ None of the:
      1. ☐ Certified copies of the priority documents have been received.
      2. ☐ Certified copies of the priority documents have been received in Application No. _____ .
      3. ☐ Copies of the certified copies of the priority documents have been received in this national stage application from the International Bureau (PCT Rule 17.2(a)).

   * Certified copies not received: _____.

Applicant has THREE MONTHS FROM THE "MAILING DATE" of this communication to file a reply complying with the requirements noted below. Failure to timely comply will result in ABANDONMENT of this application.
THIS THREE-MONTH PERIOD IS NOT EXTENDABLE.

4. ☐ A SUBSTITUTE OATH OR DECLARATION must be submitted. Note the attached EXAMINER'S AMENDMENT or NOTICE OF INFORMAL PATENT APPLICATION (PTO-152) which gives reason(s) why the oath or declaration is deficient.

5. ☐ CORRECTED DRAWINGS (as "replacement sheets") must be submitted.
   (a) ☐ including changes required by the Notice of Draftsperson's Patent Drawing Review (PTO-948) attached
      1) ☐ hereto or 2) ☐ to Paper No./Mail Date _____.
   (b) ☐ including changes required by the attached Examiner's Amendment / Comment or in the Office action of Paper No./Mail Date _____.

   Identifying indicia such as the application number (see 37 CFR 1.84(c)) should be written on the drawings in the front (not the back) of each sheet. Replacement sheet(s) should be labeled as such in the header according to 37 CFR 1.121(d).

6. ☐ DEPOSIT OF and/or INFORMATION about the deposit of BIOLOGICAL MATERIAL must be submitted. Note the attached Examiner's comment regarding REQUIREMENT FOR THE DEPOSIT OF BIOLOGICAL MATERIAL.

Attachment(s)

1. ☐ Notice of References Cited (PTO-892)
2. ☐ Notice of Draftperson's Patent Drawing Review (PTO-948)
3. ☒ Information Disclosure Statements (PTO/SB/08), Paper No./Mail Date 1/09
4. ☐ Examiner's Comment Regarding Requirement for Deposit of Biological Material
5. ☐ Notice of Informal Patent Application
6. ☐ Interview Summary (PTO-413), Paper No./Mail Date _____ .
7. ☒ Examiner's Amendment/Comment
8. ☐ Examiner's Statement of Reasons for Allowance
9. ☐ Other _____.

DETAILED ACTION

1. The Applicant's amendment, filed 28 January 2009, has been received and entered into the record, respectfully and carefully considered.

2. As a result of the amendment, claims 1, 3-4, 6, 9-11, 13, 15, 18 and 21 are amended. Claims 2, 7 and 14 are canceled. Claim 29 is a newly added claim. Claims 26-28 are withdrawn from consideration since they are non-elected claims in response to restriction/election requirement. Therefore, claims 1, 3-6, 8-13 and 15-29 are pending in the application. Claims 1, 3-6, 8-13, 15-25 and 29 have been examined.

Information Disclosure Statement

3. The information disclosure statement (IDS) submitted on 28 January 2009 was considered by the examiner.

EXAMINER'S AMENDMENT

4. An examiner's amendment to the record appears below. Should the changes and/or additions be unacceptable to applicant, an amendment may be filed as provided by 37 CFR 1.312. To ensure consideration of such an amendment, it MUST be submitted no later than the payment of the issue fee. Authorization for this examiner's amendment was given in a telephone interview with Mr. Benjamin A. Kimes (Registration No. 50,870) on 24 March 2009 and 26 March 2009. The amendment is to cancel non-elected claims and to further clarify the invention. As per MPEP 713.04, a separate interview summary form is not provided because the content of the interview has been summarized herein.

Please note in the below authorized examiner's amendment, "a hardware processor" is added to the claims 1 and 13. This newly added claim limitation is supported by page 6, paragraph [0012] and fig. 1 of the original disclosure. The supporting paragraph and figure disclose "Processor 110 may have…embedded key, page table registers and cache memory". To an ordinary skill in the art at the time of the invention, a processor has embedded key, page table registers and cache memory is a hardware processor. Thus, at least one machine is being recited and the method claims 1, 3-6, 8-12, 25 and 29 are positively tied to a particular machine that accomplishes the claimed method steps. Therefore, claims 1, 3-6, 8-12, 25 and 29 are statutory.

Furthermore, in the below authorized examiner's amendment, it removes "and electrical, optical, acoustical and other forms of propagated signals (e.g., carrier wave, infrared signals, digital signals, etc.); etc" from the instant Specification. Thus, the examiner takes the act of deleting as a disavowal.

The application has been amended as follows:

IN THE SPECIFICATION:

- Please **delete** "and electrical, optical, acoustical and other forms of propagated signals (e.g., carrier wave, infrared signals, digital signals, etc.); etc" from page 12, paragraph [0031], lines 19-20

IN THE CLAIMS:

- Please **cancel Claims 26-28**
- Please **replace Claims 1, 4, 13, 15, 16, 18, 19, 21-23 and 25** as below:

(Claim 1) (Currently Amended) A method comprising:

executing, by a hardware processor, a protected application in a protected execution environment that is provided by a trusted platform, the protected execution environment being associated with a protected section of memory that is inaccessible to direct memory access and an unprotected section of memory that is accessible to direct memory access, wherein the trusted platform includes a trusted path and an untrusted path ~~port mapped to the protected section of memory and an untrusted port mapped to the unprotected section of memory~~;

determining, by the hardware processor executing the protected application, that information is to be accessed from a subscriber identity module (SIM) device that includes a SIM card, the SIM device being physically connected with the trusted platform;

wherein the trusted path is a path between the protected application and the SIM device, the trusted path being a path through a trusted port of the trusted platform, wherein the trusted port is mapped to the protected section of memory;

wherein the untrusted path is another path between the protected application and the SIM device, the untrusted path being a path through an untrusted port of the trusted platform, wherein the untrusted port is mapped to the unprotected section of memory;

exchanging unencrypted data that includes an encryption key between the SIM device and the protected application via the[[a]] trusted path~~, the trusted path being a path through the trusted port~~, wherein the unencrypted data to be exchanged is secured from unauthorized access via properties of the trusted port; and

~~encrypting additional data using the encryption key; and~~

exchanging [[the]] encrypted data that is additional data that has been encrypted using the encryption key between the SIM device and the protected application via the[[an]] untrusted path~~, the untrusted path being a path through the untrusted port~~.

(Claim 4) (Currently Amended) The method of claim 1, wherein exchanging the encryption key includes the protected application accessing the encryption key from the SIM device, the protected application accessing the encryption key via the trusted port.

(Claim 13) (Currently Amended) A system comprising:

~~a system memory having a protected section that is inaccessible to direct memory access, an unprotected section that is accessible to direct memory access and a protected memory table that identifies the protected section and the unprotected section;~~

~~a processor having a private cache memory that has protections that prevent access to said private cache memory by unauthorized devices, and registers that identify memory pages of the system memory that are accessible only to trusted code;~~

~~a logic circuit having a trusted port mapped to the protected section of the system memory and an unprotected port mapped to the unprotected section of the system memory, the system memory, processor and logic circuit being components of a platform that is configured to provide a trusted environment for an application; and~~

~~a SIM device that includes a SIM card, the SIM device being physically connected with the platform, to exchange unencrypted data that includes an encryption key with an application executed in the trusted environment via the trusted port, wherein the unencrypted data to be exchanged is secured by the trusted port from unauthorized access, and to exchange encrypted data with the application via the unprotected port.~~

a memory having a protected section that is inaccessible to direct memory access and an unprotected section that is accessible to direct memory access;

a trusted platform to provide a protected execution environment, the protected execution environment being associated with the protected section of memory and the unprotected section of memory, wherein the trusted platform includes a trusted path and an untrusted path; and

a hardware processor to execute a protected application in the protected execution environment, wherein the trusted application to:

determine that information is to be accessed from a subscriber identity module (SIM) device that includes a SIM card, the SIM device being physically connected with the trusted port;

wherein the trusted path is a path between the protected application and the SIM device, the trusted path being a path through a trusted port of the trusted platform, wherein the trusted port is mapped to the protected section of memory;

wherein the untrusted path is another path between the protected application and the SIM device, the untrusted path being a path through an untrusted port of the trusted platform, wherein the untrusted port is mapped to the unprotected section of memory;

exchange, with the SIM device, unencrypted data that includes an encryption key via the trusted path, wherein the unencrypted data to be exchanged is secured from unauthorized access via properties of the trusted port; and

exchange, with the SIM device, encrypted data that is additional data that has been encrypted using the encryption key via the untrusted path.

(Claim 15) (Currently Amended) The system of claim 13, wherein the exchange of the encryption key includes the protected application to transmit the encryption key to the protected section of ~~system~~ memory, and the SIM device to access the encryption key from the protected section of ~~system~~ memory.

(Claim 16) (Currently Amended) The system of claim 13, wherein the exchange of the encryption key includes the protected application to access the encryption key from the

SIM device, the protected application to access the encryption key via the trusted port of the trusted platform ~~logic circuit~~.

(Claim 18) (Currently Amended) The system of claim 13, wherein the system further includes a host controller to transmit data from the SIM device to the unprotected section of ~~system~~ memory.

(Claim 19) (Currently Amended) The system of claim 18, wherein the system further includes a driver to transmit data from the unprotected section of memory to the protected application.

(Claim 21) (Currently Amended) The system of claim 13, wherein the SIM device is to read the encryption key from the protected section of memory via the trusted port of the trusted platform~~logic circuit~~.

(Claim 22) (Currently Amended) The system of claim 13, wherein the protected application is to decrypt the encrypted data using the encryption key.

(Claim 23) (Currently Amended) The system of claim 13, wherein the protected application is to authenticate the SIM device prior to the exchange of the encryption key.

(Claim 25) (Currently Amended) The method of claim 1, further comprising:

determining, by the SIM device, that the protected application is executed in the trusted execution environment~~platform~~ before exchanging the unencrypted data.

Response to Arguments

5. Applicant's argument filed 28 January 2009 have been fully considered and they are persuasive (See allowable subject matter below)

Allowable Subject Matter

6. Claims 1, 3-6, 8-13, 15-25 and 29 are allowed.

Contact Information

Any inquiry concerning this communication or earlier communications from the examiner should be directed to APRIL Y. SHAN whose telephone number is (571)270-1014. The examiner can normally be reached on Monday - Friday, 8:00 a.m. - 5:00 p.m., EST.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Y. Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/April Y Shan/
Examiner, Art Unit 2435

/Kimyen Vu/

Supervisory Patent Examiner, Art Unit 2435